Kansas Enterprise Electronic Preservation

KEEP System Policy Framework

Version 1.0

September 2010

Contents

Glossary 4

1.0 Purpose 6

1.1 Policy Adoption 6

1.2 Scope 6

1.3 KEEP System Objectives 6

2.0 Compliance 6

2.1 Open Archival Information System (OAIS) Conformance 6

2.2 Producer-Archives Interface 7

2.3 Preservation Metadata 7

2.4 Metadata Transmission 7

2.5 Trusted Digital Repository Certification 7

2.6 Compliance with requirements of Kansas Uniform Electronic Transmissions Act (Kansas Rev. Statute 16-601) 7

2.7 COBIT Compliance 7

2.8 Compliance Audit Procedure 7

3.0 KEEP System Organizational Viability 8

3.1. Roles and Responsibilities 8

3.1.1 Kansas State Historical Society 8

3.1.2 Director, KSHS State Archives and Library Division 8

3.1.3 State Archivist 8

3.1.4 State Records Board 9

3.1.5 Other Records Retention and Disposition Authorities 9

3.1.6 Electronic Records Committee 10

3.1.7 Information Technology Executive Council (ITEC) 10

3.1.8 KEEP System Operator 11

3.1.9 Organizational Leadership 11

3.1.10 Agency Records Officer 11

3.1.11 Chief Information Technology Architect (CITA) 11

3.1.12 Chief Information Technology Officers (CITO) 11

3.1.13 INFORMATION NETWORK OF KANSAS 12

3.2 Financial Sustainability 12

3.2.1 Rate Setting Process 12

3.2.2 Fee Basis 12

3.3 KEEP System Operating Principles and Procedures 12

3.3.1 General Principles 12

3.3.2 KEEP SYSTEM 13

3.4 Records Selection Criteria 13

3.5 Records Acquisition 13
3.5.1 Submission Agreements 13
3.5.2 Ingest 14
3.6 Preservation Approaches 14
3.6.1 Storage Device and Media Refreshment and Replication 14
3.6.2 Repackaging 14
3.6.3 Transformation 14
3.6.4 Viewer Technologies 14
3.6.5 Technology Neutral File Formats 15
3.6.6 Migration 15
3.6.7 Repository Software 15
3.7 Records Authentication and Integrity Protection 15
3.8 Access and Use Criteria 15
3.8.1 Access 15
3.8.2 Usage 15
3.8.3 Restrictions, Including Redaction 15
4.0 Facility Management and Operational Controls 16
4.1 Physical Controls 16
4.1.1 Site Location and Construction 16
4.1.2 Physical Access 16
4.1.3 Power and Environmental Conditioning 16
4.1.4 Water Exposure 16
4.1.5 Fire Prevention and Detection 16
4.1.6 Off Site Backup 17
4.2 Personnel Controls 17
4.2.1 Qualification of Personnel 17
4.2.2 Background Check Requirement 17
4.2.3 Training Requirements 17
4.2.4 Sanctions 18
5.0 Compliance Reviews and Other Assessments 18
5.1 Frequency 18
5.2 Qualifications of Auditor 18
5.3 Scope of Audits 18
5.4 Actions Following Audit 18
6.0 Policy Administration 19
6.1 Policy Review 19
6.2 Suggested Changes and Notice 19
6.3 Review and Comment Period 19
6.4 Final Decisions 19
6.5 Changes Outside Annual Review 19

7.0 Privacy and Data Protection 20
7.1 Protection of Confidential or Personal Identifiable Information 20
7.2 Release of Information for Criminal or Civil Matter. 20
7.3 Limitation on Liability 20
7.4 Severability. 20
7.5 Governing Law. 20
7.6 Contact Information 20
Appendix 1 Minimum Ingest Standards 21
Appendix 2 Viewer Technology 22
Appendix 3 File Formats Accepted By KEEP System 23
Appendix 4 Software Obsolescence 24

Glossary

(will be combined into single KEEP System Glossary)

Access: The OAIS entity that contains the services and functions which make the archival information holdings and related services visible to Consumers.

Archival Information Package (AIP): An Information Package, consisting of the content information and the associated Preservation Description Information (PDI), which is preserved within an ISO 14721 (OAIS) based digital repository.

Authenticity: The degree to which a person (or system) regards an object as what it is purported to be. Authenticity is judged on the basis of evidence.

Born Digital: Refers to materials that originate in digital form.

Consumer: The role played by persons or client systems who interact with OAIS services to find preserved information of interest and to access that information in detail. This can include other digital archives and/or repositories, as well as internal OAIS persons or systems.

Dissemination Information Package (DIP): The Information Package, derived from one or more AIPs, received by the Consumer in response to a request to the ISO 14721 (OAIS) based digital repository.

Fixity Information: The information which documents the authentication mechanisms and provides authentication keys to ensure that the Content Information object has not been altered in an undocumented manner.

Information Package: The content information and associated Preservation Description Information which documents the preservation of the Content Information. The Information Package has associated Packaging Information used to delimit and identify the Content Information and Preservation Description Information.

Ingest: The OAIS entity that contains the services and functions that accept Submission Information Packages from Producers, prepares Archival Information Packages for storage, and ensures that Archival Information Packages and their supporting Descriptive Information become established within to the ISO 14721 (OAIS) based digital repository.

Long-Term: A period of time long enough for there to be concern about the impact of changing technologies on the records held in the repository. For purposes of the KEEP System, long-term records are those with retention periods of 10 or more years.

Open Archival Information System (OAIS): An archive, consisting of an organization of people and systems that has accepted the responsibility to preserve information and make it available for a Designated Community. It meets a set of responsibilities, as defined in 3.1 of the ISO 14721:2003 standard that allows an OAIS archive to be distinguished from other uses of the term “archive”. The term “Open” in OAIS is used to imply that this Recommendation and future related Recommendations and standards are developed in open forums, and it does not imply that access to the archive is unrestricted.

Preservation Description Information (PDI): The information which is necessary for adequate preservation of the Content Information and which can be categorized as Provenance, Reference, Fixity, and Context information.

Producer: The role played by persons or client systems who provide the information to be preserved. This can include other OAISs or internal OAIS persons or systems.

Refreshment: A Digital Migration where the effect is to replace a media instance with a copy that is sufficiently exact that all Archival Storage hardware and software continues to run as before.

Repackaging: A Digital Migration in which there is an alteration in the Packaging Information of the AIP.

Replication: A Digital Migration where there is no change to the Packaging Information, the Content Information, and the PDI. The bits used to represent these Information Objects are preserved in the transfer to the same or new media instance.

Submission Information Package (SIP): An Information Package that is delivered by the Producer to the OAIS for use in the construction of one or more AIPs.

Technology Neutral Open Standard File Format: A technology neutral file format is one that is designed to run on multiple platforms in a variety of software applications. It is an open file format in that the design of the specification involves collaboration in an open, public environment. Technology neutral open file formats can evolve as technology changes and thereby provide a backward compatibility to older versions. Examples of technology neutral file formats are XML and PDF/A.

Transformation: A Digital Migration in which there is an alteration to the Content Information or PDI of an Archival Information Package. For example, changing ASCII codes to UNICODE in a text document being preserved is a Transformation.

Trusted Digital Repository: A trusted digital repository is one whose mission is to provide long-term access to managed digital resources; that accepts responsibility for the long-term maintenance of digital resources on behalf of its depositors and for the benefit of current and future users; that designs its system(s) in accordance with commonly accepted conventions and standards to ensure the ongoing management, access, and security of materials deposited within it; that establishes methodologies for system evaluation that meet community expectations of trustworthiness; that can be depended upon to carry out its long-term responsibilities to depositors and users openly and explicitly; and whose policies, practices, and performance can be audited and measured.

1.0 Purpose

1.1 Policy Adoption

This policy is approved by the State Records Board and implemented in conjunction with the Kansas . Information Technology Executive Council (ITEC), and may be revised and updated at any time.

1.2 Scope

This policy governs the establishment and operation of the Kansas Enterprise Electronic Preservation (KEEP) System to provide preservation processes that ensure the long-term readability, accessibility, and authenticity of electronic Kansas government records.

The mission of the KEEP System is to ensure reliable, long-term preservation and access by Kansas citizens to state government records retained for historical, legal, fiscal or administrative reasons, or for research purposes as foundations of government accountability, transparency, and public trust.

The legal authority for the KEEP System is the Government Records Preservation Act, the Public Records Act, and the State Archivist's Duties, as amended by HB 2195.

1.3 KEEP System Objectives

The objective of the KEEP System is to establish and sustain a scalable and auditable trusted digital repository infrastructure for the state of Kansas in order to preserve the readability and accessibility of electronic records across successive generations of information technology.

The KEEP System provides capabilities to ensure access to all of the electronic Kansas government records that user communities are entitled to see, and to restrict access to records to those users communities with appropriate access rights and privileges.

The KEEP System authenticates electronic Kansas government records upon request.

The KEEP System automates, to the extent possible, the capture of all required descriptive, contextual, administrative, and preservation metadata for records ingested into the KEEP System and persistently links that metadata to the electronic Kansas government records to ensure understandability of the records over time.

The KEEP System provides a mechanism for ingesting electronic records from all Producers of Kansas government records as early in the life cycle of the records as practicable.

The KEEP System maintains the chain of custody for the entire lifetime of electronic Kansas government records once they are ingested into the KEEP System.

The KEEP System interfaces with other information technology systems and networks implemented by the State of Kansas.

2.0 COMPLIANCE

2.1 Open Archival Information System (OAIS) Conformance

The KEEP System shall use the terms and concepts and support the model of information defined in the Open Archival Information System (OAIS) Reference Model approved as ISO 14721:2003. The KEEP System shall fill functional responsibilities including Ingest, Archival Storage, Access, Preservation Planning, Data Management, and Administration.

2.2 Producer-Archives Interface

The KEEP System shall conform to the Producer-archive interface - Methodology approved as ISO 20652:2006. The recommendation identifies, defines and provides specific structure to the relationships and interactions between Producer of Records and the Archive covering the initial contact between Producer and Repository until the objects of information are received and validated by the Repository.

2.3 Preservation Metadata

The KEEP System shall integrate core preservation metadata needed to support long-term preservation of electronic records and comply with the PREMIS data dictionary and supporting schemas (PREMIS 2007). PREMIS is a Digital Library Standard of the United States Library of Congress.

2.4 Metadata Transmission

The KEEP System shall adhere to the principles of the Metadata Encoding Transmission Standard (METS: 2003) in the transfer of digital content from Producers to the Repository.

2.5 Trusted Digital Repository Certification

The KEEP System will prepare to be certified as a Trusted Digital Repository once an international certification process has been finalized. The Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC: 2007) represents best current practice and thought about the organizational and technical infrastructure required for a digital repository to be considered trustworthy and capable of certification.

2.6 Compliance with requirements of Kansas Uniform Electronic Transmissions Act (Kansas Rev. Statute 16-601)

The KEEP System shall comply with all requirements of the Kansas Uniform Electronic Transmissions Act (UETA) that pertain to the delivery of digital content to the public.

2.7 COBIT Compliance

The KEEP System shall comply with selected sections of the Control Objectives for Information and related Technology (COBIT 4.1) including:

- PO 3 Determine Technological Direction; PO 8 Manage Quality; PO 9 Access and Manage IT Risks; AI 1 Identify Automated Solutions; AI 4 Enable Operation and Use; AI 5 Procure IT Resources; AI 6 Manage Changes; AI 7 Install and Accredit Solutions and Change;
- DS 1 Define and Manage Service Levels; DS 3 Manage Performance and Capacity; DS 4 Ensure Continuous Service; DS 5 Ensure System Security; DS 7 Educate and Train Users; DS 8 Manage the Service Desk and Incidents; DS 10 Manage Problems; DS 11 Manage Data; DS 13 Manage Operations;
- ME 1 Monitor and Evaluate IT Performance; ME 3 Ensure Regulatory Compliance

2.8 Compliance Audit Procedure

The KEEP System shall employ a customized audit compliance checklist that incorporates features of ISO 14721, ISO 20652, PREMIS, TRAC and COBIT and conducts a self-audit every two years.

The KEEP System Operator shall arrange for an independent third party to conduct a Compliance Audit (when this service becomes available) within one year after each self-audit and will issue a public report of the audit findings.

3.0 KEEP SYSTEM ORGANIZATIONAL VIABILITY

3.1. Roles and Responsibilities

3.1.1 Kansas State Historical Society

The Kansas State Historical Society (KSHS) encourages the effective and efficient management of state government records and provides services and resources to preserve and enable access to long-term electronic records through the KEEP System. Responsibilities of the KSHS include but are not limited to:

- Ensure technical viability of the KEEP System through preservation planning, administrativeoversight and monitoring of the KEEP System Operator.
- Manage access to permanent Kansas government electronic records and ensure compliance with the Kansas Open Records Act (KORA), other Kansas statutes, and federal law.
- Manage access to non-permanent Kansas government electronic records that have a retention period of ten years or more and ensure compliance with the Kansas Open Records Act (KORA), other Kansas statutes, and federal law.
- Ensure authorized retention and disposition rules are applied to non-permanent electronic records in the KEEP System and restrict access to the records based on written authorization and certified identification protocols.
- Provide access to records and/or execute holds on stored Kansas government electronic records upon the written request of the records Producer in the event of a public records request, litigation or investigation.

3.1.2 Director, KSHS State Archives and Library Division

The Director of the Kansas State Historical Society's State Archives and Library Division shall provide executive oversight of the KEEP System. Specific duties include:

- Sign and provide oversight for legal agreements including Memorandum of Understanding with record Producers, submission agreements, and third party contracts.
- Ensure financial sustainability and oversight of the KEEP System through approval of the three (3) year IT Management and Budget Plan submitted by the KEEP System Operator.

3.1.3 State Archivist

The State Archivist shall be accountable for all activities related to the digital preservation function of the Kansas State Historical Society. Specific duties include:

- Chair the committee that advises the State Records Board andtheInformationTechnologExecutive Council on digital preservation issues, requirements and standards.
- Prepare recommendations, in accordance with HB 2195, for preservation processes to maintain the authenticity of electronic Kansas government records and submit to the Electronic Records Committee for review and endorsement, and to the State Records Board for approval.
- Certify the authenticity of electronic government records ingested and stored in the KEEP System.
- Identify and develop digital preservation standards and best practices. Submit to the Electronic Records Committee for review and endorsement, and to the State Records Board for approval.
- Recommend fees for records authentication and other Repository services.

- Develop digital preservation cost models to determine the long-term storage costs that agencies will pay for storage of non-permanent Kansas government electronic records with an approved retention period of ten years or longer.
- Review IT Project Plans under the authority of ITEC Guideline 2400A to ensure long-term preservation requirements are adequately addressed. Specific attention shall be given to estimating the costs of digital preservation and storage services as well as ensuring new systems have State Records Board authorized records retention schedules.
- Administer the KEEP System Policy Framework by monitoring external trends and developments related to digital repositories, and by revising and updating the framework as needed to conform to national and international standards and best practices.
- Ensure compliance by state agencies in all branches of government with KEEP System digital preservation standards and requirements through the standardization of Information Package designs for specific preservation methods and file formats and the promulgation of mandatory policies, procedures, standards and metadata requirements. (See Appendix 1)

3.1.4 State Records Board

Under the authority of the Kansas Public Records Act (K.A.A. 75-3502 through 75-3504) the State Records Board is mandated to oversee "the permanent preservation of important state records and to provide an orderly method for the disposition of other state records." HB 2195 augmented the authority of the State Records Board by requiring the State Archivist to prepare and present recommendations regarding preservation processes for maintaining the authenticity of electronic records.

In addition to these roles and responsibilities the State Records Board also has the statutory authority to:

- Approve Executive Branch retention and disposition rules
- Approve Executive Branch recordkeeping plans for electronic records series
- Approve recommendations from the State Archivist based on national and professional standards for preservation processes for maintaining the authenticity of electronic Kansas government records
- Issue administrative regulations that support the KEEP System.

3.1.5 Other Records Retention and Disposition Authorities

The Legislative and Judicial Branches of Government shall be responsible for identifying business considerations and practical requirements relating to managing and preserving electronic Kansas government records and to submit these considerations to the ITEC Electronic Records Committee for review and adoption. In addition, these authorities shall have the following responsibilities:

Judicial Branch

- Approve Judicial Branch retention and disposition rules
- Approve District Court retention and disposition rules
- Approve Judicial Branch recordkeeping plans for electronic records series
- Adopt recommendations from the State Archivist based on national and professional standards for preservation processes for maintaining the authenticity of Judicial Branch records

Legislative Branch

- Approve Legislative Branch retention and disposition rules
- Approve Legislative Branch recordkeeping plans for electronic series
- Adopt recommendations from the State Archivist based on national and professional standards for preservation processes for maintaining the authenticity of Legislative records

3.1.6 Electronic Records Committee

The Electronic Records Committee (ERC) is an advisory committee to the Information Technology Executive Council (ITEC). The Committee is chaired by the State Archivist and membership is composed of legislative, judicial and executive branch agency representatives who have electronic records management and digital preservation domain knowledge and authority.

The Electronic Records Committee shall recommend and regularly review policies, guidelines, and best practices for the creation, maintenance, long-term preservation of and access to Kansas state government electronic records. Specific duties shall include but are not limited to:

- Participates in preservation planning activities and submits digital preservation policy, standards, acceptable file formats and best practices recommendations to the State Records Board and/or the Information Technology Executive Council for consideration.
- Assists in the development of procedures related to Kansas government electronic records retention and access for the review of Information Technology Project Plans under the authority of ITEC Guideline 2400A.
- Reviews recommendations developed by the State Archivist for preservation processes to ensure the authenticity of Kansas government electronic records prior to submission to the State Records Board for approval.
- Reviews annual reports from the KEEP System Operator with regard to system performance issues, adequacy of the existing information technology infrastructure for supporting the KEEP System and projected operating and capital investment costs.
- Promotes use and expansion of the KEEP System among state entities.
- Promotes education and awareness of digital preservation standards and practices across all branches of government.
- Participates in the preparation and review of proposed updates to relevant sections of the Kansas Statewide Technical Architecture.
- Participates in the preparation and review of proposed additions to the Strategic Information Management (SIM) Plan.
- Collaborates with the Kansas State Historical Society to identify and develop new records series entries to propose to the State Records Board for inclusion in the General Retention and Disposition Schedule.
- Reviews recordkeeping plans for electronic records series that have been designated by the State Records Board as requiring long-term retention.

3.1.7 Information Technology Executive Council (ITEC)

The Kansas Information Technology Executive Council (ITEC) is responsible for approval and maintenance of all enterprise information technology policies, IT project management procedures, the statewide technical architecture, and the enterprise strategic information management plan for all branches of government. Each branch also has its own information technology policies, strategic planning, and project management procedures compatible with policies at the enterprise level.

ITEC shall support the authority of the State Archivist in complying with the requirements of ITEC Guideline 2400A. In addition, it will facilitate implementation of KEEP System standards and policies of the Electronic Records Committee approved by the State Records Board.

3.1.8 KEEP System Operator

The KEEP System Operator shall have broad responsibilities for operating system, network, and security services for the Repository including facility management and operational controls. Responsibilities include but are not limited to:

- Establish and operate all components of an infrastructure sufficient to ingest, authenticate and provide access to state government electronic records with long-term value
- Report on performance of operations in meeting its obligations as a Repository including potential risks
- Plan and forecast expenditures and resources necessary to maintain the viability of the KEEP System infrastructure

3.1.9 Organizational Leadership

The director of each state government agency and the heads of all Branches, Boards, Commissions, Departments, and Divisions shall be responsible for ensuring the preservation of long-term electronic records through compliance with policies, procedures, and methodologies approved by the State Records Board and endorsed by the Information Technology Executive Council.

The director of each state government agency and the heads of all Branches, Boards, Commissions, Departments, and Divisions shall be responsible for assigning sufficient resources to ensure that digital preservation issues are taken into account in the delivery of services to the citizens of Kansas.

Organizational leadership shall be authorized to enter into agreements with the KSHS State Archives and Library Division for the transfer and storage of permanent records as well as non-permanent Kansas state government records that must be retained for ten years or longer.

3.1.10 Agency Records Officer

Agency Records Officers shall maintain a liaison with the KEEP System, the retention and disposition authority, and the KSHS Archives and Library Division.

Agency Records Officers shall be authorized to sign and submit state government records to the KEEP System in accordance with submission requirements and standards.

3.1.11 Chief Information Technology Architect (CITA)

The Chief Information Technology Architect (CITA) publishes plans and standards under the auspices of ITEC. The CITA shall be responsible for incorporating KEEP System policies and requirements into the Kansas Information Technology Architecture, Strategic Information Management (SIM) Plan, and Kansas project management training curriculum and certification processes.

3.1.12 Chief Information Technology Officers (CITO)

Branch Information Technology Officers (CITO) provide leadership and direction for state entities and their IT investment.

Each CITO shall be responsible for ensuring compliance with digital preservation policies and best practices in all systems and functions under his/her purview. Toward this end, each CITO shall designate a Digital Preservation Officer to serve on the Electronic Records Committee and to coordinate digital preservation initiatives, priorities, and methodologies within their respective branch of government.

CITOs shall advise the State Archivist of digital preservation requirements, changes in technologies, and other evolving issues in their operations.

3.1.13 INFORMATION NETWORK OF KANSAS

The Information Network of Kansas (INK) shall support public access to the KEEP System and payment portal services.

Kansas Network Consortium, Inc. (KIC) shall collect and distribute revenue for online KEEP System authentication services.

User feedback on the KEEP System shall be routinely collected and analyzed by the network manager. Feedback results and public access requirements shall be provided to the Kansas State Historical Society.

3.2 Financial Sustainability

3.2.1 Rate Setting Process

The rate setting process is done in accordance with OMB Circular A-87 and appears as part of the annual statewide cost allocation plan (SWCAP). SWCAP filings are approved each year by the federal Department of Health and Human Services Office of Cost Allocation.

Rates must be reviewed annually to ensure they are adequate for KEEP System sustainability.

3.2.2 Fee Basis

- On demand records authentication services
- Storage of other electronic Kansas state government records that must be retained for 10 years or longer
- KEEP System pre-ingestion services including design of Submission Information Packages
- Estimated digital preservation services under the authority of ITEC Guideline 2400A
- KEEP System preservation planning and archival storage services
- Customized services

3.3 KEEP System Operating Principles and Procedures

3.3.1 General Principles

- Mandatory Repository for electronic Kansas government records with enduring value and is available for other electronic records required to be retained for 10 years or longer
- Specifically designed Repository for electronic Kansas government records preservation and access that can handle a variety of formats and supports use of open source software
- Periodic self-audits and third party audits for conformance to best practices and standards
- Sufficient human, technical and financial resources to ensure sustained attention to the management and preservation of electronic Kansas government records
- Capable of integrated life cycle records management, including the scheduled transfer of government records from records Producers to the KEEP System as soon in the life cycle of the records as practicable
- Comply with federal and state requirements for digital evidence, data privacy and data security
- The long term success of the KEEP System depends upon upstream records management programs that ensure digital records are initially created in technology neutral open standard formats. Toward this end an Enterprise Records Management Model based on the requirements of ISO 15489 should be implemented to ensure that upstream records management issues bearing on digital preservation are identified and addressed in the design and implementation of records systems.

3.3.2 KEEP SYSTEM

- Records that originate in digital form or are digitized and designated to be of permanent value shall be retained in perpetuity by the KEEP System in accordance with State Records Board (and other disposition authority) requirements.
- Other records that originate in digital form or are digitized that have an authorized retention period of ten years or more shall be stored in the KEEP System
- Access to records stored in the KEEP System shall be administered in accordance with the provisions of the submission agreement.
- Producers file signed permissions for authorization to access non-permanent electronic records with a retention period of 10 years or longer. PKI shall be used to certify the authenticity of rights to access such records.
- State Archivist authenticates KEEP System records on demand
- Capability to auto-ingest records, close to the point of creation/finalization from records Producers according to scheduled records life cycle transfer protocols specified in submission agreements
- Records Producers must have approved (by their respective branch retention and disposition authority) retention and disposition instructions and complete a Submission Information Package (SIP) in order to transfer records to the KEEP System
- Agency Records Officers shall have the authority to transfer electronic state government records to the KEEP System
- KEEP System provides for future migration of the electronic records to provide preservation and access over time, including migration of file formats and periodic media renewal

3.4 Records Selection Criteria

KEEP System shall accept Kansas government records that originate and are maintained in digital form and digitized Kansas government records that have authorized retention and disposition instructions which identify them as having permanent value.

The KEEP System shall accept Kansas government records that originate or are and maintained in digital form or digitized Kansas government records that have a retention of 10 years or longer

Non-permanent electronic records with a retention period of 10 years or longer will be retained in the KEEP System until their authorized retention period expires after which they will be destroyed in accordance with approved disposition instructions

KSHS shall identify and periodically update a list of a limited number of archival preservation standard formats and support their use in the KEEP System to ensure the retrievability, usability, and authenticity of electronic Kansas government records.

KEEP System may accept government electronic records from Producers that are in proprietary and obsolescent file formats

3.5 Records Acquisition

3.5.1 Submission Agreements

KEEP System shall implement State Records Board requirements for the transfer of legal custody of records of permanent value to the Kansas State Historical Society

KSHS shall negotiate agreements with Kansas government agencies/entities (Producers) that produce business records with a permanent value and non-permanent electronic records with retention periods of 10 years or longer

Submission agreements for permanent as well as non-permanent electronic records shall include any and all restrictions for access based upon statutes or regulations

3.5.2 Ingest

The KEEP System accepts Kansas government electronic records through a process called Ingest. The Ingest process shall use standardized information packages and protocols for the actual transfer of electronic records from a records Producer to the KEEP System.

Core OAIS ingestion protocols that are supplemented with features customized for the KEEP System shall be developed and implemented. (See Appendix 1).

The KEEP System shall support the automated, semi-automated, and manual transfer of Kansas government electronic records that meet the selection and acquisition criteria from records Producers and records management systems and business applications.
Electronic Kansas government records shall be transferred to the KEEP System through secure protocols: Web Portal, File Transfer Protocol (FTP), LTO Magnetic Tape, DVD or CD.

3.6 Preservation Approaches

Technology obsolescence is inevitable as new computers, processing methodologies, and storage devices displace current ones. Typically, there is a window of time between five to ten years after displacement has occurred before the pace of technology obsolescence begins to escalate sharply as vendor support declines. Complete technology obsolescence that results in digital content no longer being accessible or usable is inevitable unless addressed within the time window referenced above. The KEEP System will maintain evidence of any preservatin actions performed on records in the repository.

The KEEP System shall use a variety of approaches to mitigate technology obsolescence:

- Storage device and media refreshment and replication
- Migration repackaging
- Migration transformation
- Viewer technologies
- Technology neutral file formats
- Open source software

3.6.1 Storage Device and Media Refreshment and Replication

The KEEP System shall preserve the bit streams of electronic Kansas government records through periodic storage device and media refreshment and replication.

3.6.2 Repackaging

The KEEP System shall preserve evidence of any preservation activities that result in changes to KEEP Repackaging Information.

3.6.3 Transformation

The KEEP System will employ Transformation to convert Archival Information Packages (AIPs) to new archival storage file formats as they become available.

3.6.4 Viewer Technologies

The KEEP System shall use Viewer Display Technologies to render electronic records stored in proprietary file formats and provide access to static, non-processible renditions of the records. (See Appendix 2)

3.6.5 Technology Neutral File Formats

The KEEP System shall adopt technology neutral file open standard formats for archival storage (See Appendix 3).

During the Ingest process, non-legacy proprietary file format records will be transformed to an archival storage format where such tools are available.

Producers will be encouraged to implement these same technology neutral open standard file formats in their operational records systems. Digital records in these formats are "preservation ready" so no transformation activities will be required during Ingest.

3.6.6 Migration

The KEEP System shall mitigate technology obsolescence through migration unless emulation tools are established and widely used and become a digital preservation best practice. (See Appendix 4)

3.6.7 Repository Software

Sustainability of the KEEP System will be supported wherever possible through the design and use of community-supported open source software and systems.

3.7 Records Authentication and Integrity Protection

The KEEP System shall protect the authenticity of Kansas government electronic records by requiring records Producers to authenticate records at the time of transfer and by creating and maintaining preservation activity and other metadata that supports an electronic chain of custody.

3.8 Access and Use Criteria

3.8.1 Access

The KEEP System shall ensure access to electronic Kansas government records that have been retained for long-term preservation and use by the public, legislators, courts, and Kansas agencies.

The KEEP System shall enable access to its holdings for different user communities and sets of security rights.

The KEEP System shall comply with Kansas Open Records Act exemptions and other state and federal laws restricting access to Kansas government records.

The KEEP System shall comply with access requirements of ADA Section 508 and related statutes as well as ITEC Policy 1210.

3.8.2 Usage

KEEP System shall support persistent access to Kansas government electronic records of enduring value through multiple access points, including the Kansas.gov portal and the portal of the Kansas State Historical Society.

KEEP System shall disseminate electronic records in selected technology neutral open standard formats.

The KEEP System shall support authorized Producer access to Kansas government electronic records in its physical but not legal custody through a portal restricted to Kansas government employees with certified authorization.

3.8.3 Restrictions, Including Redaction

KEEP System shall redact or otherwise restrict public access to Kansas government electronic records based on the restrictions identified in the submission agreement. This includes but is not limited to redaction using the appropriate technology tools in accordance with the current redaction policy of the KSHS.

KEEP System will comply with legal holds issued by the records Producers on electronic records stored by the KEEP System by temporarily suspending all disposal actions associated with the records.

4.0 Facility Management and Operational Controls

4.1 Physical Controls

4.1.1 Site Location and Construction

The location and construction of the facility housing the KEEP System will be consistent with Tier 4 facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, will provide robust protection against unauthorized access to the KEEP System.

4.1.2 Physical Access

The facility that houses the KEEP System will implement physical access controls to reduce the risk of equipment tampering and malicious manipulation of the software system.

At a minimum, physical access controls must:

- ensure that no unauthorized access to the hardware is permitted,
- ensure that all removable media and paper containing sensitive plain-text information regarding access to or operation of the system and its configuration is stored in secure containers, be manually or electronically monitored for unauthorized intrusion at all times
- ensure that an access log is maintained and inspected periodically and require two-person physical access control to both the database and storage subsystems
- ensure physical security systems (e.g., door locks, vent covers) are functioning properly.

A person or group of persons will be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance will be maintained. If the facility is not continuously attended, the last person to depart will initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

4.1.3 Power and Environmental Conditioning

The KEEP System will have backup capability sufficient to automatically lock out input, finish any pending actions and record the state of the equipment before lack of power or environmental conditioning causes a shutdown.

The equipment will be installed so that it is not in danger of exposure to water, e.g., placement on tables or elevated floors. Moisture detectors will be installed in areas susceptible to flooding.

4.1.4 Water Exposure

This policy makes no provision for prevention of or exposure of KEEP System equipment to water beyond that called for by practices that are commercially reasonable within the industry for Tier 4 facilities. Equipment will be installed so that it is not in danger of exposure to water, e.g., racks or elevated floors. Moisture detectors must be installed in areas susceptible to flooding.

The KEEP System Operator that has sprinklers for fire control will have a contingency plan for recovery should the sprinklers malfunction or cause water damage outside of the fire area.

4.1.5 Fire Prevention and Detection

This policy makes no provision for prevention of exposure of the KEEP System to fire beyond that called for by practices that are commercially reasonable within the industry for Tier 4 facilities. An automatic fire extinguishing system will be installed in accordance with local code.

The KEEP System Operator must have a contingency plan which contemplates and addresses damage by fire.

4.1.6 Off Site Backup

System backups, sufficient to provide recovery from system failure will be made on a periodic schedule that provides for complete recovery of the system and data. At least one backup copy must be stored at an offsite location separate from the KEEP System. Only the latest backup is required to be retained. The backup will be stored at a site with physical and procedural controls commensurate with that of the operational system.

4.2 Personnel Controls

4.2.1 Qualification of Personnel

The KEEP System Operator will implement and comply with personnel and management policies sufficient to ensure the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this policy.

4.2.2 Background Check Requirement

At a minimum the KEEP System Operator staff with direct access to the repository will pass a background investigation covering the following areas:

- employment
- education
- place of residence
- law enforcement and
- references.

The period of investigation must cover at least the last five years for each area, with the exception of the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree must be verified. Any personnel who fail an initial or periodic background check must not serve in a trusted role.

The Director, KSHS Archives and Library Division may request conduct of periodic background checks at their discretion.

4.2.3 Training Requirements

All personnel performing duties related to the operation of the KEEP System will receive comprehensive training appropriate to their roles, and the training will be documented. Training will be conducted in the following areas:

- security principles and mechanisms;
- all software versions in use on the system including special storage media;
- all duties they are expected to perform;
- disaster recovery and business continuity procedures; and
- provisions of the law and this policy.

All persons responsible for KEEP System operations will be made aware of changes in the operations appropriate to their roles. Any significant change to the operations will have a training awareness plan, and the execution of the plan must be documented. Examples of changes are software or hardware upgrades, changes in automated security systems and relocation of equipment. In any event, the KEEP System Operator will review operational requirements with persons performing significant or trusted roles at least once a year.

The KEEP System Operator will document the training program, identity of all personnel who receive training and the level of training completed.

4.2.4 Sanctions

The KEEP System Operator will take appropriate administrative and disciplinary actions against personnel who have performed actions not authorized by law, this policy or who have been negligent in performing their duties in the operation of the KEEP System.

5.0 Compliance Reviews and Other Assessments

5.1 Frequency

The KEEP System Operator shall submit to and pay for compliance reviews applicable to trusted digital repositories and file the review report with the State Records Board.

Once every three years an external review by a competent third party must be conducted. An internal review performed by the KEEP System Operator must be prepared annually except in those years in which a third party audit is performed.

5.2 Qualifications of Auditor

A compliance auditor shall be qualified to conduct a compliance review pursuant to those standards recognized by this policy law and must be sufficiently familiar with the best practices of a trusted digital repository. The auditor must be thoroughly familiar with the requirements of TRAC and other applicable standards as identified in Section 2 of this policy.

The auditor shall have a contractual relationship for the performance of the review, and the auditor shall be sufficiently separated legally and organizationally from the KEEP System Operator to provide an arms-length, unbiased, independent evaluation. To ensure this, the selected auditor shall be approved by KSHS.

5.3 Scope of Audits

Audits shall be conducted in accordance with Kansas law, this policy, other applicable standards and with TRAC. The purpose of the compliance audit is to verify that the KEEP System Operator complies with all of the requirements of Kansas law, this policy and standards for trusted digital repositories.

5.4 Actions Following Audit

If audit findings report any material noncompliance with Kansas law, this policy, applicable ISO standards or TRAC, the following actions shall be performed:

- the compliance auditor must note the discrepancy in writing;
- the compliance auditor must notify the parties in section 3 of the discrepancy and
- the party responsible for correcting the discrepancy shall propose a remedy in writing, including an expected time for completion, to the State Archivist

Depending upon the nature and severity of the noncompliance, the KEEP System Operator may be required to suspend ingestion of any new content until the non-compliance is remedied. If the severity of the noncompliance is determined by the Electronic Records Committee not to warrant lapse of ingesting new content, it may negotiate a timetable and project plan for the successful completion of the remedy.

The final order concerning the remedy and the status of the KEEP System Operator will be made by the management of the KSHS (or it could name Pat's position, or say the State Records Board in conjunction with the State Archivist, etc.).

6.0 Policy Administration

6.1 Policy Review

This policy will be reviewed by the State Records Board on an annual basis.

6.2 Suggested Changes and Notice

Suggested changes to this policy will be communicated to the State Records Board on or before October 1 each year. Such communication must include a description of the change, a change justification and contact information for the person requesting the change. On or before October 31st of each year, the State Records Board will provide notice of proposed changes under consideration.

6.3 Review and Comment Period

Interested parties may file comments concerning the proposed changes with the State Records Board on or before November 31 each year. After receipt of the comments, the State Records Board will use its best efforts to review the comments and provide its approved policy changes, if any, to Information Technology Executive Committee (ITEC) by December 31 each year.

6.4 Final Decisions

Final decisions on the proposed changes to this digital preservation policy are at the sole discretion of the State Records Board, with the support and advice of the State Archivist and ITEC Electronic Records Committee If a proposed change is adopted as a result of the policy review, a notice of the change will be given to all branches of government and all parties for whom Submission Agreements with the KEEP System exist.

6.5 Changes Outside Annual Review

Notwithstanding the foregoing, if, in the judgment of the State Records Board or the State Archivist, it is determined changes to the policy should be made prior to the annual review, the State Records Board reserves the right to modify the policy upon notification of the proposed changes to all branches of government and all parties for whom a Submission Agreement exists.

7.0 Privacy and Data Protection

7.1 Protection of Confidential or Personal Identifiable Information
TBD

7.2 Release of Information for Criminal or Civil Matter

Only the State Archivist may authorize disclosure of protected information to a law enforcement agency or other duly-authorized agent in a criminal or civil matter and only under the following circumstances: when (1) required to be disclosed by law, governmental rule or regulation or court order; or (2) authorized by the producing entity. Any request for such disclosure of private and/or confidential information must be made in accordance with applicable law.

7.3 Limitation on Liability
TBD

7.4 Severability
Should it be determined that one section of this policy is invalid, the other sections will remain in effect until the policy is updated. The process for updating this policy is described in section XXX.

7.5 Governing Law
The laws of the United States of America and the State of Kansas will govern the enforceability, construction, interpretation and validity of this policy.

7.6 Contact Information
Communication to the State Records Board should be addressed to:

Name
Address 1
Address 2

Appendix 1 Minimum Ingest Standards

At a minimum the KEEP System Ingest process will include:

- Virus check and quarantine
- Specification of permanent or non-permanent digital records
- Authenticated legal or physical custody agreement with records Producer
- Digital record content
- Authentication of transfer of Submission Information Packages (SIP)
- Notification of SIP receipt to Producer
- Transmission integrity validation
- Version of software used to create or store digital record content
- File format validation
- Required descriptive, structural, administrative and preservation metadata
- Procedures for conversion to an Archives Information Package (AIP), including normalization as appropriate
- Retain a copy of the original bit stream ingested before normalization
- Specification of normalization storage standards

The KEEP System will protect the integrity of digital records by the use of hash digests, digital signatures, and time stamps to validate that no change has occurred.

Appendix 2 Viewer Technology

File formats provide critical information about special operations (e.g., compression), instructions on how to interpret the digital content (e.g., image, text, audio), specifications of a software application required to process the bit stream, and identification of non-printing characters that represent rendering specifications, such a type font. They are essential in the creation, use, storage, and preservation of digital records but transparent to users.

Many file formats can be characterized as proprietary, native formats that are application dependent and therefore can only be opened and used by the original software application. Proprietary file formats are subject to technology obsolescence as vendors displace them with new file formats and cease supporting the older ones. Over time, these formats become "legacy file formats" because tools to convert them to newer formats are not available or may be prohibitively expensive to develop.

Fortunately, viewer display technology can render representations of many electronic records without using the native applications originally used to create them. This rendering capability includes display viewing and printing functionality that can run on multiple technology platforms.

Viewer display technologies, which currently enable this rendering capability for more than 500 native file formats, can be used to render electronic records embedded in legacy file formats and applications. This is only a short term solution because in the future at some point current viewer technologies may not be supported.

Appendix 3 File Formats Accepted By KEEP System

File formats accepted by the KEEP System include:

- Text
- Extended American Standard Character Information Interchange (ISO 8859-1)[1]
- Open Document Format (ODF)
- Portable Document Format/Archives (PDF/A)
- Extensible Markup Language (XML)
- Hypertext Markup Language (HTML)
- Comma Separated Values (CSV) for spreadsheets

Photographic Images

- Lossless JPEG 2000 (Joint Photographic Experts Group)

Scanned Images

- PDF/A (Portable Document Format Archives)
- PNG (Portable Network Graphics)

Vector Graphics

- SVG (Scalable Vector Graphics)

Geospatial

- PDF/E (Portable File Format Engineering)

Audio

- BWF (Broadcast Wave Format)

Digital Video

- JPEG 2000 (Motion JPEG 2000)

In some instances it may be appropriate to Ingest digital content in native legacy formats for which no software tools currently exist for normalizing them in archival preservation formats. In such instances the KEEP System will support the bit preservation (rendering will be accomplished by a compatible viewer) through media and device renewal until new tools are available that can normalize them into archival preservation formats..

[1] It can be argued that Unicode, which is an International Standard that can support text in more than 65,000 languages, should be the recommended standard for text. However Unicode requires 16 bits as opposed to the 8 bits of Extended ASCII. The first 8 bits of Extended ASCII and Unicode are identical but transforming Extended ASCII to Unicode would add 8 "null" bits to each alphanumeric, which has the net effect of doubling the storage space requirements with no appreciable gain.

Appendix 4 Software Obsolescence

A software application is required to interpret the bit streams underlying electronic records and render these representations of 1s and 0s into a human useable form. In this sense all electronic records are software dependent. Software applications are vulnerable to technology obsolescence as vendors develop new platforms and products and discontinue support of others. Over time software applications that vendors no longer support cannot open, retrieve, and use electronic records.

Two approaches may be considered to mitigate application software application obsolescence: migration and emulation. Migration is the process for repeated conversion or transformation of digital records from one technology platform to a more stable one. No special computer code is required in migration because it relies on interoperable, backwardly compatible technology neutral open standard formats. In contrast, emulation replicates the functions and capability of a software package by emulating the hardware and operating system on which it originally ran. Because emulation replicates the original software used to create and use digital records, the digital records remain in their original native file format. Unlike emulation, migration is an established and widely used approach to mitigate technology obsolescence.